United Nations A/54/213

General Assembly

Distr.: General
10 August 1999
English
Original: English/Arabic/
Russian/Spanish

**Fifty-fourth session**
**Item 71 of the provisional agenda***
**Developments in the field of information and telecommunications in the context of international security**

# Developments in the field of information and telecommunications in the context of international security

## Report of the Secretary-General

Contents

| | | Page |
|---|---|---|
| I. | Introduction | 2 |
| II. | Replies received from Governments | 2 |
| | Australia | 2 |
| | Belarus | 2 |
| | Brunei Darussalam | 3 |
| | Cuba | 3 |
| | Oman | 6 |
| | Qatar | 7 |
| | Russian Federation | 8 |
| | Saudi Arabia | 11 |
| | United Kingdom of Great Britain and Northern Ireland | 11 |
| | United States of America | 11 |

* A/54/150.

99-23597 (E) 200899 300899

# I. Introduction

1. The General Assembly, by paragraphs 2 and 3 of its resolution 53/70 of 4 December 1998, entitled "Developments in the field of information and telecommunications in the context of international security", invited all Member States to inform the Secretary-General of their views and assessments on the following questions: (a) general appreciation of the issues of information security, (b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources, and (c) advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality, and requested the Secretary-General to submit a report to it at its fifty-fourth session.

2. On 19 March 1999, the Secretary-General addressed a note verbale to Member States requesting them to provide their views pursuant to the invitation of the Assembly. The replies received from Governments are reproduced below.

# II. Replies received from Governments

## Australia

[Original: English]
[2 June 1999]

1. Australia chaired the Group of Experts of the Organisation for Economic Cooperation and Development (OECD) which prepared the OECD Guidelines for the Security of Information Systems. Australia also chairs the OECD Working Party on Information Security and Privacy which has responsibility, *inter alia*, for monitoring the need for information security. Australia participates in the development by the International Organization for Standardization (ISO) of security standards for information technology. Domestically, Australia has detailed processes for the security of government information and Standards Australia, in conjunction with Standards New Zealand, has developed a joint standard on information security management based on a British standard. The Australian Government and industry are currently working together on steps to protect the national information infrastructure. Australia has legislated to protect telecommunications systems from interception, interference and some forms of misuse.

2. The objective of information security, as defined in the OECD Guidelines for the Security of Information Systems and used by Australia, is: "... the protection of the interests of those relying on information systems from harm resulting from the failure of availability, confidentiality and integrity".

3. With the convergence of technologies, the objective can be extended to cover telecommunications systems that are a specific type of information system. Any interference with or misuse of information systems will have an impact on either availability, confidentiality or integrity. There is a danger of developing technology-specific definitions in a rapidly changing environment.

4. Australia would not support the Department for Disarmament Affairs of the United Nations Secretariat as the appropriate body to develop international principles on the security of global information and telecommunications systems. Telecommunications and information infrastructure impact on issues of trade, economic development and societal well-being, as well as law enforcement and national security. Principles and guidelines on these issues have already been developed in other forums, such as OECD, ISO and the International Telecommunication Union (ITU) from broader perspectives than those proposed in General Assembly resolution 53/70. In addition, international bodies such as the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) and the Centre for International Crime Prevention are addressing computer crimes issues. Australia does not see benefit in other arms of the United Nations duplicating work which is being done elsewhere in relation to computer security or misuse. Australia would support a proposal to develop an information resource of the work being undertaken in other forums.

## Belarus

[Original: English]
[25 May 1999]

1. The Republic of Belarus fully supports General Assembly resolution 53/70 of 4 December 1998, entitled "Developments in the field of information and telecommunications in the context of international security". The vigorous application of new information technologies and means of telecommunication expands the broadest opportunities for accelerated development of world civilization. At the same time, as specified by the Assembly in resolution 53/70, "these technologies and means can potentially be used for purposes that are inconsistent with

the objectives of maintaining international stability and security and may adversely affect the security of States".

2. Adoption of Assembly resolution 53/70 is timely and relevant because it draws the attention of the international community to the potential use of information technologies in the conduct of war and the need to prevent the application of new information technologies and means in a military context, where they could be compared with weapons of mass destruction. Moreover, with the adoption of General Assembly resolution 53/70, there is a possibility of specifically considering the problem of international information security, including unauthorized interference with, or misuse of, information and telecommunications systems and information resources. Finally, it is advisable to develop and agree on a concept of international information security and international legal principles aimed at enhancing the security of global information and telecommunications systems and preventing information terrorism and criminality.

## Brunei Darussalam

[Original: English]
[7 June 1999]

With regard to General Assembly resolution 53/70 of 4 December 1998, entitled "Developments in the field of information and telecommunications in the context of international security", the Permanent Mission of Brunei Darussalam has the honour to convey the following views of the Ministry of Defence of Brunei Darussalam:

> "The Ministry of Defence, as a Ministry responsible for National Defence, accepts that security of information in this era of information technology is important. For this Ministry, any form of information that can be used and may threaten national security in its transmission is considered important. However, because of its links to information technology and because it is also under the purview of other ministries in the country, the Ministry of Defence will cooperate with the relevant agencies to fulfil the desires of the resolution. In order to protect and guarantee the security of international communications, the responsibility should not be considered as beyond the jurisdiction of the International Court of Justice".

## Cuba

[Original: Spanish]
[28 June 1999]

### General appreciation of the issues of information security

1. The widespread use of information technologies in practically all spheres of human activity, which has been called the "computerization of society" and which many refer to as the "information era" owing to the world's increasing dependence on information systems, poses new security problems that require very serious consideration not only by every State but also by the entire international community.

2. For this reason, the United Nations is the appropriate forum for discussing relevant ways and means of dealing with the potential dangers that the use of new information and telecommunications technologies for non-peaceful purposes may pose for international security.

3. In addition, the necessary measures must be taken to make these technologies available for the development of all States, particularly underdeveloped countries that lack sufficient resources to develop such technologies by themselves.

4. On the other hand, globalization is already a reality in the field of information and telecommunications, and distances no longer pose an obstacle to the exchange of information; at the same time, the systems that facilitate this exchange of information are exposed to increasing security risks. It must be emphasized that globalization entails a level of standardization that makes it easier to interfere with these systems.

5. We must not forget that we are talking about technologies that originate in developed countries, among which the United States of America, the world's largest hegemonic Power, particularly in the field of information and telecommunications, enjoys a pre-eminent position that enables it to impose technological standards that facilitate the use of information and telecommunications systems as a means of aggression.

6. In contrast, the underdeveloped countries have no alternative other than to accept these technologies in order to survive under the new conditions. Most of the time, these countries are not fully aware of the risks involved and they often do not make sufficient use of security arrangements, services or mechanisms. This leads to the vulnerability of information systems which, owing to the widespread use of

information and telecommunications technologies in all spheres of human development, can give rise to situations that jeopardize international security.

7. Cuba is very pleased to have an opportunity to consider the item in the General Assembly pursuant to the initiative that resulted in the adoption by consensus of Assembly resolution 53/70. Cuba is mindful of the importance of the item and will participate actively in the assessments called for in that resolution.

**Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources**

8. The world in which we live is witnessing an unprecedented increase in the use of information and telecommunications technologies, which unfortunately has made it possible to use them for hostile purposes in order to carry out the aggressive policies that some States have adopted towards other States.

9. In this regard, it should be pointed out that the development and popularity of global networks, particularly the Internet, have had important consequences. In spite of their increased use, information and telecommunications systems are still operated on a purely cooperative basis. This is important, since the voluntary nature of the Internet is at once the source of its strength and its greatest weakness.

10. The common set of rules for ensuring the effective and enhanced operational security of global networks is voluntary owing to the fact that countries have not adopted uniform legislation concerning the operation of information networks.

11. However, since association with these global networks is optional, it is reasonable to argue that any rule of conduct governing such networks should be part of the agreement of association, and that the violation of such rules, regardless of the existing legal infrastructure, may result in sanctions.

12. Security of information includes the protection of its confidentiality (information should be accessible only to those who are entitled to use it), protection of information against unauthorized modification (integrity), and protection of systems against denial of services (availability) and against unauthorized access.

13. In this context, some basic criteria must be taken into consideration:

(a) Users are responsible for their own conduct; in other words, non-authorized access to a computer or non-authorized use of a network is an explicit violation of the rules of conduct, no matter how weak the means of protecting information systems may be;

(b) Organizations that use these technologies are responsible for their employees' appropriate use of them and should therefore elaborate security policies to that end, as well as measures and procedures that ensure their control. Likewise, each country should establish appropriate mechanisms to ensure that organizations based in their territory comply with these requirements;

(c) Providers of computer services and networks are responsible for maintaining the security of the systems that they operate. They are also responsible for informing users of their security policies and of any change in such policies;

(d) Vendors and suppliers of systems are responsible for providing reliable systems that include adequate security controls. The vendor or supplier must evaluate each system in terms of security controls before the system is put on the market. Each product must describe the security features included in it. Vendors and suppliers of systems are obliged to repair defects in the relevant parts of the systems that they sell or distribute free of charge;

(e) Users, suppliers of services and vendors of software and hardware are responsible for cooperating in the provision of security. It is to be hoped that each site will notify the other if it discovers that a site is being penetrated, and that they will assist each other in taking measures to address security violations. Such assistance can include the tracing of connections, detection of violations and legal assistance.

14. The main objectives of a person who attacks information networks are to:

(a) Obtain, alter or destroy information. This is undoubtedly the main objective of most attackers;

(b) Hack into other people's computers and use them as if they were the authorized users;

(c) Gain a point of departure for further attacks. Systems may be invaded for the sole purpose of launching new attacks from those systems;

(d) Denial of service, that is, making information unavailable to someone who needs it and is entitled to use it;

(e) Gain publicity, which is very useful in the case of Web servers.

15. The misuse of information and telecommunications systems and information resources, especially when such

systems and resources are used by some States to carry out their policies of interference in the affairs of other States, is an infringement of the sovereignty and independence of the affected States and creates centres of tension that may pose a serious threat to international security.

16. The persistent efforts of States to achieve political ends that serve their national interests entail the misuse, according to established international norms, of, *inter alia*, radio and television stations with a view to destabilizing the constitutional order of other States considered to be enemies.

17. Cuba is an example of a State affected by the policies mentioned in the preceding paragraphs. To give an idea of the seriousness of the matter, Cuba for decades has been subjected to aggression by United States radio and television, which is part of the steadfast policy of aggression by the world's foremost military, economic and political power whose declared aim is to overthrow the Government of Cuba.

18. To this end, for example, until April 1999 there were a total of 17 stations situated in the territory of the United States of America that broadcast subversive information to Cuba.

19. Every day, between 288.5 and 306.5 hours of medium-wave, short-wave and FM radio signals were broadcast; 2,084.5 hours every week and, if we add to that the television signals transmitted every week, this would amount to a total of 2,089 hours.

20. In most cases, the information incites Cuban citizens to commit acts of civil disobedience and engage in destructive and terrorist acts.

21. Cuba has always been in favour of solving differences between States on the basis of equality and respect for their national sovereignty and independence and has expressed this publicly on various occasions. This position remains unchanged.

**Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality**

22. Without a doubt, the development of new information technologies calls for parallel efforts to ensure the progressive development of international law in this area, including the elaboration of an adequate legal framework that would enhance the security of information systems.

23. The task will not be easy, if we take into account the fact that there are still questions that will require the elaboration of generally accepted definitions in order to facilitate the subsequent codification of new principles that would help achieve objectives in the area of security.

24. The very nature of global networks goes beyond the jurisdictional limits of each country; in many cases, this makes it impossible to rely on geographical frontiers. In addition, the unequal development of States, among other factors, makes it rather difficult to establish uniform international regulations that can be generally applied to all countries that share these technologies.

25. Nevertheless, we would not be starting from scratch, since there already exist generally accepted principles and international legal instruments that have been agreed and adopted by States in various multilateral forums in keeping with recent technological progress. These principles and instruments would be very useful in consolidating or developing new international principles to enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.

26. To mention a few relevant examples of such agreements, Cuba considers that the following should be taken into account:

(a) General Assembly resolution 110 (II) of 3 November 1947, which condemns propaganda designed to provoke or encourage any threat to peace, breach of the peace, or act of aggression;

(b) The International Telecommunication Convention, adopted at Nairobi in 1982, as well as the relevant international legal instruments adopted by the United Nations Educational, Scientific and Cultural Organization and the International Telecommunication Union;

(c) The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, which were adopted by the General Assembly and which stipulate that such activities should be carried out in conformity with international law and in a manner compatible with the development of mutual understanding and the strengthening of friendly relations and cooperation among States and peoples in the interest of maintaining international peace and security;

(d) The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, the annex to which contains provisions on the protection of confidential information that could also serve as a useful reference for elaborating the aforementioned principles.

27. Finally, and as part of the leading role that the United Nations should play in the analyses that may be made of this subject, Cuba considers that the Organization should, *inter alia*, recognize that every country has the right to protect its information and telecommunications systems with secure protection systems, and recommend that Member States adopt laws that sanction the development and dissemination of computer viruses and other harmful programmes. In addition, legally binding multilateral agreements that prohibit aggression against information and telecommunications systems could be concluded within the framework of the United Nations. Consideration could also be given to the conclusion of agreements that guarantee the use of the new technologies being developed for peaceful purposes, and their availability to all States.

## Oman

[Original: Arabic]
[22 June 1999]

1. The Sultanate's Telecommunications Authority is not responsible for providing information to subscribers but only supplies the networks and technologies that facilitate access to information systems.

2. As a provider of networks and technologies, the Authority has a general appreciation of the issues of information security. It can be said that there is a possibility that the technologies provided by the Authority may be used by unauthorized parties to gain access to information and that this may have adverse consequences.

3. As a provider of telecommunications services, the Authority does not normally have responsibility for the security of the information of subscribers who must themselves establish the necessary safeguards to meet the security requirements of their information. The Authority may, however, restrict access to information in the public domain through some services, such as the Internet.

4. In connection with basic notions related to information security, the regulations in effect in the Sultanate, and especially the copyright regulations, characterize information as having material and moral value and thus provide it with legal protection. By means of this principle, it is possible to define the basic notions relating to information security. The most important are as follows:

(a) Illicit interception of information and data;

(b) Illicit entry to computer systems;

(c) Spying and eavesdropping on data and information;

(d) Violation of the privacy of others or of their right to confidentiality;

(e) Provision of data or electronically stored documents of whichever kind;

(f) Destruction, alteration and diversion of data;

(g) Collection and diversion of information;

(h) Leaking of information and data;

(i) Trespass on computer programs by modification or counterfeiting;

(j) Illicit copying of programs in violation of intellectual property rights;

(k) Theft and use of network addresses;

(l) Alteration, augmentation or deletion of information in an original message in transmission before it reaches the addressee;

(m) Introduction of viruses and tampering with network content;

(n) Actual (physical) destruction of equipment and buildings.

5. Possible solutions to enhance the security of information systems include the following:

(a) Security-related education for personnel concerning the dangers and their prevention;

(b) Access control; that is, the issuance of permits of various kinds to those authorized to have access to information in particular categories;

(c) The use of numerical identifiers (numerical signatures, numerical certifications) for communication between genuine users;

(d) Encryption of both hardware and software;

(e) Use of firewalls to prevent the entry of information that has been tampered with;

(f) Use of anti-viruses.

6. The Sultanate expresses the hope that international principles will be developed to enhance the security of global information systems, particularly since it has introduced an Internet service and has thus become exposed to the dangers relating to information security.

## Qatar

[Original: English]
[10 June 1999]

The concerned authorities in the State of Qatar have communicated the following information regarding their views and assessments in respect of paragraphs 2 and 3 of General Assembly resolution 53/70 of 4 December 1998:

(a) *General appreciation of the issues of information security*. General appreciation of the issues of information security could be achieved by the exchange of expertise and by understanding the risk of unauthorized interference, as well as its effect on security and financial aspects;

(b) *Definition of basic notions related to information security*. The basic notions for promoting security are those steps that have to be followed to ensure ways and means for the communication of information, as well as the challenges that take place unexpectedly, as illustrated in tables 1 and 2 below, which list the necessary steps at all stages to ensure the security of information, in addition to the new challenges in that respect;

(c) *Principles which would enhance security of communications*. The promotion of security information could be achieved by pursuing progress in the means of transmitting information, and the following points are the most important in respect of promoting the security of communications, taking into consideration the high financial cost involved:

(i) Use of irregular communication protocols which could be designed specifically for the exchange of certain information;

(ii) Use of a coding system that is designed for a specific purpose and should not use programs that are manufactured in commercial quantities;

(iii) Adopt changes which have different timing and coding.

Table 1
**Network security solutions**

| *Security steps* | | |
|---|---|---|
| *Threat* | *Security solution* | *Function* |
| Data intercepted, read or modified illicitly | Encryption (DES, RSA algorithm) | Encodes data to prevent tampering |
| A valid user gets access to data he or she is not authorized to access | Access control software | Assigns and manages user privileges |
| A user misrepresents his or her identity in order to commit fraud | Authentication | Technique that includes encryption software and token cards to verify the identities of both sender and receiver |
| Unauthorized user on one network gains access to another | Firewall | Filters and prevents certain traffic from entering the network or server |
| Hacker exploits holes in the server's operating system in order to gain access to and tamper with data | Operating system tools | Plugs known holes in the operating system |

Table 2
**Security challenges**

| *The changes* | *The challenges* |
|---|---|
| *Today's network:* | *Security is threatened because:* |
| Includes many more portable computers | Portable computers are easy to steal |
| Has more wireless connections | Wireless links can be tapped more easily |
| Is more dispersed geographically | Remote sites are harder to protect |
| Links a wider variety of platforms | User forgets a password or writes down multiple passwords |
| Interconnects increasingly with public networks, such as the Internet | Hackers stalk the public networks |
| Uses UNIX computer systems more often | UNIX operating system has particular vulnerabilities |

## Russian Federation

[Original: Russian]
[9 June 1999]

### General comments

1. One of the characteristic features of the current stage of world scientific and technological progress is the global information revolution — the rapid development and universal application of the most recent information technologies and global means of telecommunication. Affecting all areas of the vital activities of States, the information revolution is opening up new opportunities for developing international cooperation and is creating a global information area in which information is becoming an extremely valuable part of a country's wealth and its strategic resources.

2. At the same time, it is becoming clear that, along with the positive aspects of that process, there is also a real threat that developments in the information field can be used for purposes that are inconsistent with the objectives of maintaining international stability and security and complying with the principles of the sovereign equality of States, the peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs and respect for human rights and freedoms.

3. The use of the most recent information technologies to build up the military potential of countries alters the global and regional balance of forces and gives rise to tension between traditional and emerging centres of power and influence.

4. A fundamentally new area of confrontation in the international arena is in the making, and there is the danger that scientific and technological developments in the field of information and communications might lead to an escalation of the arms race. In such a situation, both the national security of individual States and the overall system of international collective security at the regional and global levels are affected.

5. We are referring to the creation of an "information weapon", the use of which, depending on the level of a society's information technology and the vulnerability of its vital structures, can have devastating consequences, comparable to the effect of weapons of mass destruction. It is obvious that such a weapon can be used by terrorist, extremist or criminal groups, as well as by individual lawbreakers.

6. Thus, the universality, secrecy or impersonality of the information weapon, the possibility of its widespread use across national borders and its economy and overall efficiency make it an extremely dangerous means of exerting influence, and contemporary international law has virtually no means of regulating the development and application of such a weapon.

7. In this connection, there is an obvious need for international legal regulation of the worldwide development of civilian and military information technology, and for the formulation of a coordinated international policy on information safety that meets the needs of international security.

### Proposed measures

8. The basis for the international community's further efforts in this area can be General Assembly resolution 53/70, entitled "Developments in the field of information and telecommunications in the context of international security", which the Assembly adopted by consensus on 4 December 1998; the draft resolution on the subject was introduced by the Russian Federation.

9. The General Assembly must adopt resolutions on the question of information security with a view to reducing the threat of the use of information for terrorist, criminal or military purposes.

10. It is essential that the joint consideration of the situation in the area of information security should be continued in order to identify all existing positions and

views and to take them into consideration in common efforts to advance the concept of information security.

11. As common approaches and trends are identified, work should begin on the development of international principles (e.g., a regime, a code of conduct for States) with a view to strengthening international information security. At the outset, these principles could take the form of a multilateral declaration; they would subsequently be incorporated into a multilateral international legal instrument. Work in this area should also be conducted within the framework of the Conference on Disarmament at Geneva.

12. At the same time, the international community should consider and adopt the aforementioned principles as a package, that is, bearing in mind threats of a military, terrorist or criminal nature and with a view to applying those principles to both the military and civilian spheres.

### Main threats to international information security

13. The main threats to international information security are:

(a) Creation and use of means of influencing or damaging another State's information resources and systems;

(b) Deliberate use of information to influence another State's vital structures;

(c) Use of information with a view to undermining a State's political and social system; psychological manipulation of a population for the purpose of destabilizing society;

(d) Actions by States to dominate and control the information area, prevent access to the most recent information technologies and create a situation in which other States are technologically dependent in the information sphere;

(e) Actions by international terrorist, extremist or criminal associations, organizations, groups or individual lawbreakers that pose a threat to a State's information resources and vital structures;

(f) Formulation and adoption by States of plans or doctrines providing for the possibility of waging information wars and capable of provoking an arms race and causing tension in relations among States, and of leading to information wars per se;

(g) Use of information technologies and means to the detriment of human rights and freedoms in the field of information;

(h) Uncontrolled transboundary dissemination of information, in contravention of the principles and norms of international law and the domestic legislation of specific countries;

(i) Manipulation of information flows, disinformation and concealment of information with a view to undermining a society's psychological and spiritual environment and eroding traditional cultural, moral, ethical and aesthetic values;

(j) Information expansion and acquisition of a monopoly over another State's national information and telecommunication infrastructures, including conditions for their operation in the international information area.

### Main tasks and objectives for developing an international information security regime

14. There is a need to create an international legal basis for:

(a) Identifying the characteristic features of and classifying information wars;

(b) Identifying the characteristic features of and classifying information weapons, as well as methods and means that may be regarded as information weapons;

(c) Restricting traffic in information weapons;

(d) Prohibiting the development, dissemination or use of particularly dangerous types of information weapons;

(e) Preventing the threat of information wars;

(f) Prohibiting the use of information technologies and means for hostile purposes and, in particular, against agreed categories of facilities;

(g) Acknowledging that the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction;

(h) Creating conditions for the equitable and safe international exchange of information, based on a balance of interests of the individual, society and the State;

(i) Preventing threats of the use of information technologies and means for terrorist or other criminal purposes;

(j) Preventing the threat of the use of information technologies and means to influence social consciousness with a view to destabilizing a society and State;

(k) Developing a procedure for mutual notification and prevention of the unsanctioned use of information to influence other States;

(l) Creating a mechanism to settle conflict situations in the area of information security;

(m) Creating an international system for certifying information technologies and means (including software and hardware) with a view to guaranteeing their information security;

(n) Developing a system of international cooperation among law-enforcement agencies with a view to preventing crime in the information sphere;

(o) Creating a mechanism for monitoring compliance with the conditions of the international information safety regime;

(p) Harmonizing national legislation in order to ensure information safety.

**Basic notions related to international information security**

15. Basic notions related to international information security include:

(a) *Information area.* The sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and telecommunications infrastructure and information itself;

(b) *Information resources.* Information infrastructure (hardware and systems for creating, processing, storing and transmitting information), including data files and bases, and information and information flows;

(c) *Information war.* Confrontation between States in the information field, with a view to damaging information systems, processes and resources and vital structures, and undermining another State's political and social systems, as well as the mass psychological manipulation of a State's population and the destabilization of society;

(d) *Information weapon.* Means and methods used with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defence, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State;

(e) *Information security.* Protection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information per se with respect to its characteristics, such as integrity, objectivity, accessibility and confidentiality;

(f) *Threat to information security.* Factors that endanger the basic interests of the individual, society and the State in the information area;

(g) *International information security.* The state of international relations that excludes the violation of international stability and the creation of a threat to the security of States and the international community in the information area;

(h) *Illegal use of information and telecommunications systems and information resources.* Use of telecommunications and information systems and resources without the relevant authorization or in violation of the applicable rules, legislation or norms of international law;

(i) *Unsanctioned interference in information and telecommunications systems and information resources.* Interference in the collection, processing, accumulation, storage, search for, dissemination or use of information with a view to disrupting the normal functioning of information systems, or the violation of the integrity, confidentiality or accessibility of information resources;

(j) *Vital structures.* A State's facilities, systems and institutions, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defence system, law-enforcement agencies, strategic information resources, scientific establishments and scientific and technological developments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations);

(k) *International information terrorism.* The use of telecommunications or information systems and resources, or the influencing of those systems or resources, in the international information area for terrorist purposes;

(l) *International information crime.* The use of telecommunications or information systems and resources, or the influencing of those systems or resources, in the international information area for illegal purposes.

## Saudi Arabia

[Original: Arabic]
[27 May 1999]

Many governmental and private institutions, in every State that relies increasingly on electronic information systems, have made progress in the field of information technology. Commensurate with such progress, however, is the increase in the number of acts intended to disrupt, jeopardize and tamper with those information systems that are carried out by international parties with a view to destruction and terrorism. This causes damage to the economy, to society and to security. It is essential that international principles and laws be put in place to counter the threat to, and abuse of, the security of information, and to combat and criminalize such international acts. Those who commit such acts must be brought to justice and punished by the international organizations concerned.

## United Kingdom of Great Britain and Northern Ireland

[Original: English]
[30 May 1999]

### General

1. Global connectivity of information-based systems has now reached the point where many, if not all, States face a potential threat to significant elements of their critical infrastructure from electronic attack by criminals and terrorists. While the danger from electronic attack is probably low at the moment, it will increase over time as public and private sectors alike become increasingly dependent on computer systems that are increasingly interlinked. Furthermore, because systems are linked internationally, the threat is a transboundary one. Criminal and terrorist attempts to penetrate our systems for malicious purposes therefore present a challenge to all Members of the United Nations. Thus, the United Kingdom of Great Britain and Northern Ireland welcomes moves to consider means, both unilateral and multilateral, by which we might seek to protect the integrity of information-based critical infrastructure against such attacks.

### Domestic action

2. To this end, in January 1999, Her Majesty's Government announced steps to minimize the risk of electronic attack on the United Kingdom's critical national infrastructure. Domestic measures include:

(a) Ensuring that within Government, all critical systems are identified and that the protection of those systems is effectively managed and audited;

(b) Working with the private sector to develop measures which keep pace with the level of risk and to ensure adequate standards of protection for the key systems falling within the critical national infrastructure;

(c) Raising awareness and standards of information security more generally in the private sector by pursuing existing initiatives to promote best practice.

### International action

3. At the same time, transboundary connectivity means that attacks on systems in other States can have a spillover effect on the United Kingdom's own critical national infrastructure and that terrorist and criminals operating from a third country could seek to attack systems in the United Kingdom. The United Kingdom therefore recognizes that international cooperation is essential to combat the threat of malicious attack and is looking to develop existing dialogues on these issues with its international partners. These include work in the Group of Eight High-Tech Crime Group on mutual legal assistance, and in the Council of Europe on a convention on cyber crime.

4. The United Kingdom considers that the United Nations should monitor work in these and other forums with a view to evaluating in due course the type of substantive actions it might usefully contribute in this field. These might include the development of international principles to enhance the security of global systems and help combat information terrorism and criminality.

## United States of America

[Original: English]
[20 May 1999]

### General appreciation of the issues of information security and definition of basic notions

1. The United States of America believes that information security is a broad and complex topic encompassing many factors and affecting many diverse activities of individuals, groups and Governments. Although the general topic includes aspects that relate to international peace and security (the work of the First Committee), it also includes technical aspects that relate to global communications, as well as non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation and other issues that

are considered in the Second or Sixth Committee. The actions and programmes of Governments are by no means the only appropriate focus, for information security also involves important concerns of individuals, associations, enterprises and other organizations active in the private sector.

**International security aspects**

2. During armed conflict, nations have employed various techniques associated with information security. Radio-frequency jamming and electro-magnetic countermeasures are two obvious examples; such techniques have a long history. In the future, it will be important for military forces to protect their own data links and other computer-related systems. Further, Member States need the capacity to restore essential information systems in the event that a natural disaster or catastrophic emergency disables key communications facilities or other data networks in the public and private sectors. Information security also extends to the protection of information related to military capabilities and other aspects of national security.

**Economic, trade, and technical factors**

3. Information security encompasses the need to protect scientific research of a commercial character, as well as production technology and other types of proprietary data (e.g., marketing plans and customer service information).

4. Information security is also associated with the need to enforce international agreements on intellectual property (such as video and audio material, as well as computer software), so as to protect it from unauthorized copying and sale. Protection of privacy is yet another aspect of information security, that is, ensuring the security of personal and commercial information transmitted via the public international network or over private data links.

5. On a technical level, regulations of the International Telecommunication Union and the activities of national counterparts ensure compatibility of electronic signals, appropriate use of the electro-magnetic spectrum and broad reliability of the International Network. These functions likewise apply to satellites that provide a wide range of services, such as voice and data relay, as well as locator data and other information used for air and sea navigation and for search and rescue services. Further, design and safety standards provide crucial assurance to manufacturers and users of electronic devices, including computers. All of these regulatory and administrative functions can be identified within the broad concept of information security.

**Law enforcement and anti-terrorist cooperation**

6. Widespread reliance on information-based technologies has resulted in an unprecedented degree of global connectivity and interdependence, with the result that many aspects of national and international activity, public and private sector alike, theoretically can be put at risk by criminal or terrorist misuse.

7. While the degree of dependence on information technology may vary from State to State, the breadth of activities that rely on such communications — economic, commercial, industrial, educational, legal — means that all States potentially are vulnerable to the consequences of criminal exploitation. Moreover, this dependence can be expected to increase as such technologies become increasingly central to the stable operation of Governments as well as to the maintenance of key global commercial and communications systems sustaining interaction between States.

8. The United States therefore views the criminal misuse of information technology as a challenge to the interests of all States and shares the concerns expressed by others that we seek to promote appropriate means, unilaterally and multilaterally, in order to ensure the integrity of our resources that are dependent upon information technology.

9. The United States likewise views any unlawful intrusion or attempt to disrupt or alter any aspect of its national information systems as a potential danger to its critical national infrastructure and thus as a threat to its national interests. The United States, recognizing the potential seriousness of this threat, has initiated at a national level, long-term, public and private programmes designed to safeguard its critical national infrastructure. The United States, however, also recognizes that, with the increasingly global interdependence of many of these essential infrastructures, the success of its national efforts to safeguard its information-based systems ultimately will depend in part upon the level of security afforded by those systems beyond its borders to which it is linked.

10. Therefore, the United States believes that all States must take the national steps necessary to ensure both the integrity of their domestic information systems and that the criminals or international terrorists operating within their national borders who attempt to disrupt those systems can be prosecuted to the fullest extent of the law. It is incumbent upon each State to take action to ensure that its information systems are reliable and as safe as possible from criminal misuse or denial of service, and that information systems can be quickly restored should system interruptions occur.

11. United States criminal law prohibits interference with United States information infrastructures. The United States urges all States to review their domestic legal statutes to ensure that they provide appropriately for the prosecution of actions related to criminal or terrorist misuse of information systems. The United States has found it necessary repeatedly to amend its computer-related statutes in order to improve them and to meet new problems.

### Advisability of developing international principles

12. As previously noted, information security is a broad and complex topic. It has many dimensions that relate to each other in extremely complicated ways. Given the clear need to analyse all aspects of information security and reach a thorough understanding of how they interact, it would be premature to formulate overarching principles pertaining to information security in all its aspects. Instead, the international community needs to do a substantial amount of systematic thinking before going further. To facilitate this, Member States should seek ideas and insights from a broad range of experts in our respective Governments and societies.

13. It is already obvious, however, that international cooperation is essential in order to combat effectively the novel and complex issues raised by information terrorism and criminality. Currently, there are several ongoing, multilateral efforts addressing international cooperation issues. The Council of Europe is examining a draft convention on cyber crime; the Group of Eight High-Tech Crime Group is looking at measures regarding mutual legal assistance and related high-tech crime issues; the Organization of American States also has established a group to study such areas; and the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders is examining related issues in a United Nations context.

14. All of these ongoing efforts have merit and should definitely be allowed to develop and bear fruit. It would be highly unwise for the General Assembly to formulate strategies or direct activities that might pre-empt or interfere with the work of the international community that is already under way.